Abstract

A process for transmitting sequences of signals/data from a transmitter to a receiver and for authenticating the sequences of signals/data consists of a precalculation phase and of a communication phase in which the signals are transmitted together with the checking sums. In the precalculation phase, a pseudo-random sequence is first generated by means of a cryptographic algorithm from a time-variable parameter and other initialization data. Non-overlapping sections (z(1) of a sequence (z) having each m bits are associated to signals (s(i)), wherein i = 1, 2, ... n, of a signal storage. Further non-overlapping m bit sections (t(i)) of the remaining sequence are selected for coding numbers (1, 2, ... MAX). The transmitter transmits the initialisation information and the time-variable parameters to the receiver and the receiver calculates the pseudo-random sequence (Z) and checks the received authentication token (T). The transmitter accepts the received signals as being authentic when the received authentication tokens match the calculated ones.